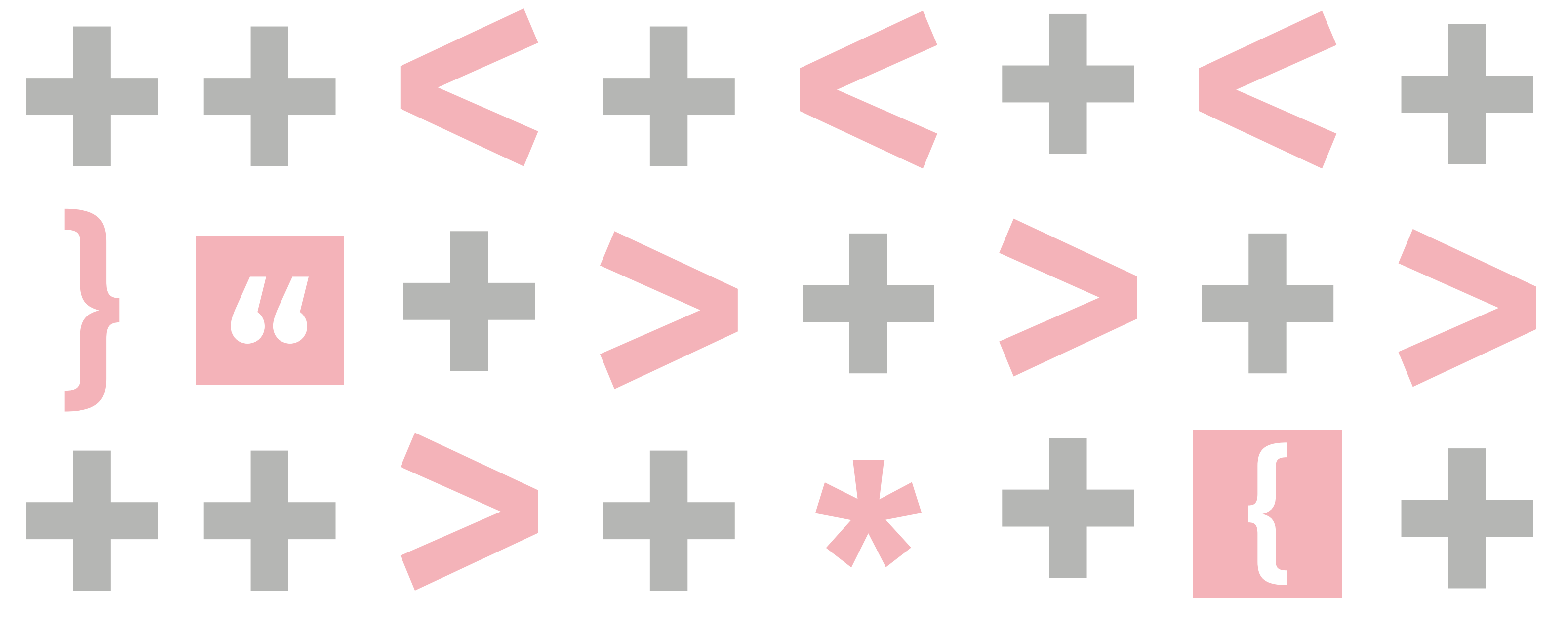
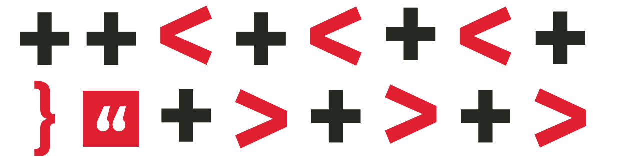


Vulnerabilidades reportadas por el K+LAB de Karisma a entidades públicas en 2020





Vulnerabilidades reportadas por el K+LAB de Karisma a entidades públicas en 2020

Autores:

Andrés Velásquez

Stéphane Labarthe

Revisión:

Carolina Botero

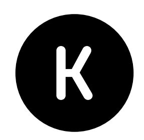
Pilar Sáenz

Diseño editorial:

Hugo A. Vásquez

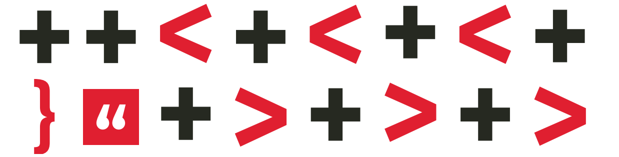


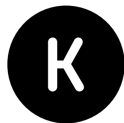






Índice





Presentación

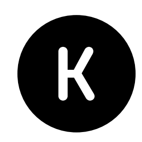
En el presente informe se hace un compendio de las vulnerabilidades encontradas y reportadas responsablemente por el Laboratorio de seguridad y privacidad digital K+LAB de Karisma durante el año 2020.

Como es bien sabido, este año estuvo marcado por la pandemia. En Colombia tanto el gobierno nacional como los de las regiones, enfocaron parte de sus esfuerzos en crear soluciones digitales como complemento a los controles establecidos para manejar la emergencia. Al margen de si estas soluciones tecnológicas fueron efectivas o no, el hecho de que giren en torno a a la recolección masiva de datos personales y de datos generados por los dispositivos (como la localización en los celulares) hizo que durante este período de tiempo el K+LAB movilizara sus esfuerzos para hacer veeduría ciudadana a dichas aplicaciones o soluciones tecnológicas. El objetivo era verificar que el tratamiento de los datos recolectados se hiciera de manera responsable y segura.

Esta veeduría, realizada usando técnicas no intrusivas y de reconocimiento pasivo, permitió encontrar vulnerabilidades que ponían en alto riesgo los datos de las personas usuarias, además dejó ver la improvisación y el afán en el despliegue de estas soluciones, la falta de auditorías y el bajo control de calidad en los procesos de desarrollo.

Además de la revisión de las aplicaciones y tecnologías desarrolladas por el Estado en el contexto de la pandemia, el K+LAB encontró una grave vulnerabilidad en la página de Migración Colombia que se suma a la de la página de la Cancillería, reportada por el portal La Silla Vacía el 15 de enero de 2021 y que demuestra debilidades que requieren atención integral inmediata en los sistemas conexos a las relaciones exteriores del Gobierno Colombiano.

Este informe solo se enfoca en las vulnerabilidades encontradas en el software auditado, sin embargo, los ejercicios e investigaciones hechas por el K+LAB mues-

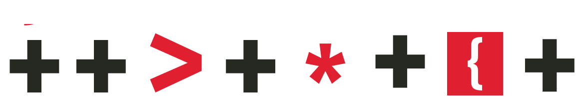


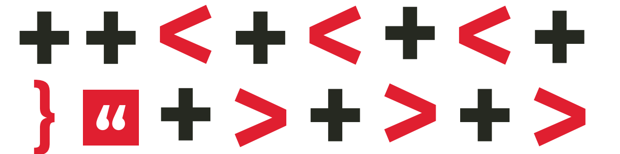


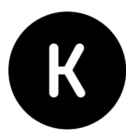
tran también varios casos donde el uso de la tecnología se hizo de manera irresponsable e ingenua, despreciando la necesidad de transparencia e información, la privacidad de las personas usuarias y los parámetros científicos para hacer rastreo de contactos. En esta línea, El K+LAB de Karisma hizo análisis al sistema de rastreo con identificadores de publicidad del departamento de Antioquia y a las "notificaciones de exposición" hechas por la alcaldía de Bogotá a través de publicidad geo referenciada en Facebook e Instagram.

En todos estos casos, el K+LAB hizo reportes responsables de las vulnerabilidades encontradas a las entidades encargadas de los desarrollos tecnológicos, enviando informes completos, socializando los hallazgos y esperando la corrección de los problemas encontrados antes de publicar reportes generales donde no se dan detalles de las vulnerabilidades encontradas.

Estos reportes y estos ejercicios están hechos con la idea de propiciar un ecosistema con rutas claras para que personas investigadoras de seguridad digital, y en principio cualquier persona, puedan reportar vulnerabilidades o amenazas que pongan en riesgo tanto la infraestructura tecnológica como los datos de las personas que interactúan con los sistemas digitales del Estado. Cómo lo explicamos en un informe en 2019, queda demostrado que contar con una ruta de coordinación de vulnerabilidades es necesario, importante y útil en el manejo y la respuesta a incidentes de seguridad informática en el país. El Gobierno debe redoblar esfuerzos para crear esta ruta y alentar su uso para el bien de toda la población.







Vulnerabilidades e incidentes reportados en 2020

CoronApp-Colombia

Transmisión de datos sensibles en texto plano (uso de HTTP)
CWE: 319
Fecha de reporte: 7 de abril de 2020
Fecha de corrección: 22 de abril 2020
Fecha de publicación: 17 de abril de 2020
Referencias: https://web.karisma.org.co/coronapp-medellin-me-cuida-y-calivalle-corona-al-laboratorio-o-como-se-hackea-coronapp-sin-siquiera-intentarlo/
Notas:

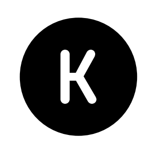
- La aplicación no usaba TLS (HTTPS) sino HTTP para comunicarse con el API. Todos sus datos (incluyendo datos personales) se transmitían sin cifrar y a la vista de cualquier observador pasivo.

Ausencia de autorización en endpoint de la API
CWE: 862
Fecha de reporte: 7 de abril de 2020
Fecha de corrección: 22 de abril de 2020
Fecha de publicación: 17 de abril de 2020
Referencias: https://web.karisma.org.co/coronapp-medellin-me-cuida-y-calivalle-corona-al-laboratorio-o-como-se-hackea-coronapp-sin-siquiera-intentarlo/
Notas:

- Esta vulnerabilidad permitía a un atacante extraer datos personales y sensibles de las personas usuarias de la aplicación a través del API.
- Era posible enumerar y automatizar la extracción de los datos debido a que el parámetro de consulta en el endpoint era secuencial.
- Para el momento en el que se hizo el reporte de esta vulnerabilidad la aplicación ya tenía más de un millón de descargas lo cual puso en riesgo una cantidad de datos importante.

Formulario Medellín Me Cuida

Ausencia de autorización en integración con EPM (Empresas Públicas de Medellín)
CWE: 862
Fecha de reporte: 17 de abril de 2020
Fecha de corrección: 23 de abril de 2020





Fecha de publicación: 30 de abril de 2020
Referencias: https://web.karisma.org.co/que-dice-que-hace-y-que-es-lo-que-realmente-hace-medellin-me-cuida/
Notas:

- Esta vulnerabilidad permitía sin ningún tipo de autenticación o autorización, consultar los datos personales y sensibles de las personas usuarias de los servicios de EPM solo con su número de contrato.
- Los número de contrato son secuenciales por lo tanto era posible enumerar y automatizar la extracción de los datos.

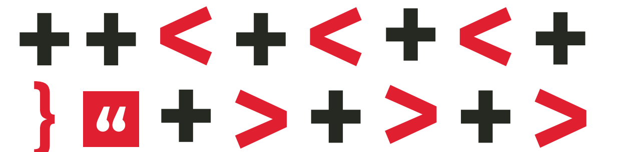
CaliValle Corona

Ausencia de autorización en 2 endpoints de la API
CWE: 862
Fecha de reporte: 16 de abril de 2020
Fecha de corrección: N/A
Fecha de publicación: 21 de abril de 2020
Referencias:
https://web.karisma.org.co/que-dice-que-hace-y-que-es-lo-que-realmente-hace-calivalle-corona/
Notas:

- Una de las vulnerabilidades permitía consultar todos los datos de una persona usuaria con su número de cédula, lo cual sumado a la cantidad de datos que recogía la aplicación resultaba muy peligroso, por ejemplo, la recolección desmesurada de la ubicación de las personas usuarias permitía saber sus movimientos con solo conocer su número de cédula.
- Ambas vulnerabilidades permitían a un atacante modificar la consulta a la API de tal forma que no solo era posible enumerar y automatizar la extracción de datos sino que se podían fabricar consultas para extraer todos los datos en una sola conexión.

GABO (Bogotá Cuidadora)

Transmisión de datos sensibles en texto plano (uso de HTTP)
CWE: 319
Fecha de reporte: 9 de junio de 2020
Fecha de corrección: N/A
Fecha de publicación: junio 24 de 2020
Referencias: https://web.karisma.org.co/rastreo-digital-en-bogota/



K

Notas:

- La aplicación no usaba TLS (HTTPS) sino HTTP para comunicarse con el API. Todos sus datos se transmitían sin cifrar y a la vista de cualquier persona observadora pasiva.

Página de Migración Colombia

Ausencia de autorización en el API de agendamiento de citas
CWE: 862
Fecha de reporte: 13 de noviembre de 2020
Fecha de corrección: 19 de noviembre de 2020
Fecha de publicación: 21 de enero de 2021
Referencias:
Notas:

- Esta vulnerabilidad daba acceso total al API usado por la página de Migración Colombia sin ningún tipo de autenticación o autorización, lo cual dejaba expuesta la información de más de 800.000 personas usuarias.
- Uno de los Endpoints del API vulnerable alojaba más de 4000 documentos sensibles.

Análisis

1. **Las entidades públicas no parecen tener la práctica de realizar auditorías de los sistemas informáticos, esto evita que actúen preventivamente incluso frente a vulnerabilidades más bien simples.**

   De las 7 vulnerabilidades relacionadas en este documento 5 son problemas de autenticación y autorización en las APIs hechas a la medida para cada aplicación o página. Y aunque la muestra es pequeña para afirmar que hay un patrón con este tipo de vulnerabilidades en sistemas del Estado colombiano, si se confirma una tendencia general que habla del creciente riesgo que representan los problemas de seguridad en las APIs para las organizaciones.

   Por la naturaleza de las auditorías que se hacen en el K+LAB (no intrusivas y pasivas) las vulnerabilidades que se encuentran son las más evidentes, las que flotan en la superficie, las que en una auditoría más profunda deberían ser encontradas el primer día. Por lo tanto, hay que deducir que a estos sistemas no se les hizo una auditoría antes de salir a producción, a pesar de que son diseñados para gestionar datos sensibles y se podía anticipar un tráfico importante.

La mayoría de las soluciones analizadas en 2020 se presentaron como instrumentos del manejo oficial de la pandemia, se apoyaban con publicidad, aprovechaban el miedo al contagio y la necesidad de las personas de movilizarse, trabajar durante las cuarentenas o viajar a medida que se relajaron las medidas. Con eso en mente, su diseño no podía improvisarse, debía estar pensado para custodiar una gran cantidad de datos personales. De hecho, incluso en el caso de Migración, se podía anticipar que sería usado por cientos de miles de personas, toda vez que es parte del trámite para solicitar la cita en el proceso de las visas para extranjeros.

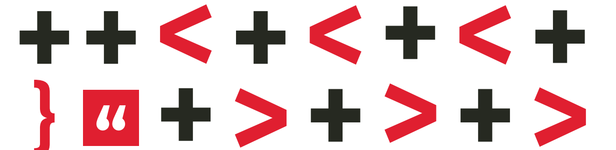
2. **No percibimos capacidad interna para atender los reportes de fallas de seguridad digital en las entidades, lo que tampoco les permite responder oportunamente y crea preguntas sobre su capacidad para entender y hacer seguimiento en esta materia a sus sistemas informáticos.**

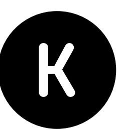
   Excepto en el caso de CoronApp-Colombia que fue desarrollada en la Agencia Nacional Digital, aunque con apoyo de la empresa privada, y Medellín Me Cuida, cuyo desarrollo estaba a cargo de EPM empresa industrial y comercial del Estado, en las reuniones que el equipo de profesionales del K+LAB, sostuvieron con las personas responsables de las entidades públicas para presentar los informes, fue evidente que aunque tenían a su cargo el sistema, el conocimiento del mismo y la capacidad para responder e incluso entender lo que sucedía estaba tercerizada y tercerizado había estado el desarrollo de las soluciones tecnológicas.

   Esto que no es a priori condenable -es incluso positivo si se tiene en cuenta que las entidades en general no pueden crear la capacidad para desarrollar cualquier tipo de sistema-, si debe ser cuestionado si al interior no hay capacidad para entender la tecnología que les desarrollan y los riesgos que ella puede suponer. Personal con este tipo de conocimiento puede aportar a la capacidad de las entidades públicas para reaccionar con prontitud a los reportes de esta naturaleza. Esta ausencia también acentúa los efectos de la falta de auditorías, pues significa que las entidades no tienen información para prevenir y evitar en lo posible estas fallas ni alguien que pueda atender el tema.

3. **Las vulnerabilidades encontradas sugieren que el diseño de estos sistemas informáticos es tercerizado y no es de buena calidad, a pesar de que se desarrollan para el Estado y gestionan datos personales.**

   Aparte de la aparente ausencia de control de calidad, al menos en forma de au-





ditorías, las vulnerabilidades en las APIs que se analizaron también dan cuenta de un diseño de baja calidad que es realizado por privados usualmente por encargo de la entidad pública.

Adicionalmente, la presencia de estas vulnerabilidades sugiere que los diseños no tuvieron en cuenta los modelos de amenazas, ni discriminan los datos sensibles de los que no lo son, por ejemplo.

Todas las vulnerabilidades en APIs aquí relacionadas fueron catalogadas como CWE-862: Missing Authorization, es decir, todas están basadas en que no hubo ninguna forma de autorización para acceder a algún recurso (o a todos) de la API que termina así devolviendo información privada o personal de quienes la usan.

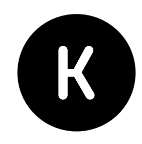
Las otras dos vulnerabilidades reportadas en este documento se refieren al no cifrado de datos en las comunicaciones de estas APIs, en palabras sencillas, usar HTTP, en vez de usar HTTPS. Este es un descuido mayúsculo, pues no solo usar HTTPS no cuesta nada si se quiere, sino que adicionalmente hoy es imposible desconocer que HTTPS es un estándar mínimo en la implementación de soluciones web o aplicaciones que se conectan con una API. Que se encuentren este tipo de vulnerabilidades en sistemas tan críticos demuestra que su despliegue fue como mínimo descuidado e irresponsable.

Aunque es claro que ningún software está exento de tener vulnerabilidades, en procesos y estándares de desarrollo de software siempre se definen lineamientos que buscan evitar introducir vulnerabilidades tan evidentes como las descritas en este informe.

4. El afán convirtió el prototipo en el producto y con ello se desconocieron garantías importantes.

Las vulnerabilidades encontradas en nuestros análisis sugieren, por lo menos para los sistemas acá mencionados, que no hubo una metodología clara de desarrollo y que se hizo de afán. La pandemia obligó a tomar medidas de urgencia y a desplegar soluciones de salud pública en tiempos récord, sin embargo, esto no puede ser un cheque en blanco para la experimentación, sobre todo cuando se involucran derechos fundamentales.

Si bien la emergencia justifica acelerar los tiempos, no es la excusa para des-





conocer las garantías. Otras soluciones como las vacunas o los ventiladores, debido a la pandemia se desarrollaron y desplegaron en tiempo récord, pero con procesos de ensayo, pruebas y evaluaciones. Sin embargo, todo esto fue ignorado en el caso de las aplicaciones que analizamos donde lo que se acogió fue la idea de que el software se construye con base en la experimentación en vivo, concepto muy arraigado en la cultura de las startups de Silicon Valley pero que no puede ser la lógica que guíe la solución oficial que atiende un problema de salud pública y pone en riesgo derechos fundamentales.

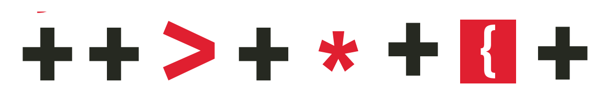
Aunque es cierto que la experimentación por sí misma no es el problema, ignorar las garantías por el afán sí lo es. Es claro que la experimentación es clave cuando se está prototipando una idea, también es cierto que el prototipo es un ensayo que se mantiene pequeño y limitado, que no se pretende masificar hasta que sea una solución robusta.

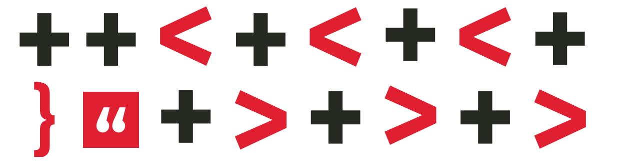
A pesar de los importantes riesgos para la privacidad, para muchas personas la emergencia justificaba desplegar soluciones de este tipo y en ese caso podrían haber justificado ensayar con prototipos en ambientes controlados, sujetos a evaluación y mecanismos de reporte que soportan una implementación (o no) posterior. Sin embargo, en el caso del gobierno colombiano parece que hace carrera que el prototipo sea el producto y con ello se adopta una aproximación que no aborda los efectos negativos de la tecnología. Vale la pena recordar que como cualquier otra herramienta, la tecnología puede producir efectos indeseados que son reales y se materializan en inseguridad digital, amenazas a la privacidad, aumento de la discriminación a poblaciones tradicionalmente vulneradas, escalamiento de violencias o amenazas a la democracia. Por tanto, tener desarrollos confiables y respetuosos de los derechos de las personas es una obligación del Estado.

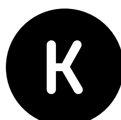
5. Es necesario aclarar lo que se entiende por incidentes que deben ser reportados a la autoridad y desarrollar mecanismos de información a las posibles víctimas.

Finalmente, en todos nuestros ejercicios animamos a las entidades a reportar las fallas a la Superintendencia de Industria y Comercio como autoridad de protección de datos. Aunque no se puede afirmar que las vulnerabilidades efectivamente se explotaron, dejan en evidencia que hubo una brecha de seguridad que pudo afectar a cientos de miles, y en ocasiones, incluso a millones de personas.

No comprobamos exhaustivamente que no se hicieran los respectivos reportes







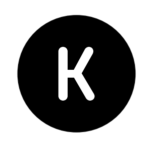
a la autoridad, pero a finales de 2020 solicitamos a la Agencia Nacional Digital, responsable de la aplicación CoronApp-Colombia, que nos informara si otras organizaciones o personas habían reportado vulnerabilidades, la forma como los habían atendido y la fecha en que reportaron esto a la SIC. la respuesta a esa solicitud de información apunta a que la entidad consideró nuestro reporte una amable alerta pero no activó la obligación legal de la ley 1581 de 2012.

Si no se están activando las alertas existentes en la ley mucho menos se está informando a las posibles víctimas y se abren preguntas sobre la forma como las entidades actúan para mitigar los riesgos que crearon. El gobierno nacional debe aclarar el alcance de la obligación legal y trabajar para desarrollar las acciones que deben desplegarse después de estos reportes pues hoy en día lo que prima es echarle tierra al asunto.

6. La veeduría ciudadana hace que la seguridad, la privacidad y la calidad de los desarrollos mejore.

Los reportes responsables y los seguimientos hechos por el K+LAB en el 2020 contribuyeron con la protección de los datos de millones de personas, no solo porque las posibles brechas que las vulnerabilidades aquí relacionadas pudieran dejar sus datos en manos de actores maliciosos sino también porque los informes que entregamos y socializamos con las entidades encargadas mostraban, en muchos de casos, problemas adicionales de privacidad como la excesiva cantidad de permisos que pedían las aplicaciones o la inclusión de rastreadores de terceros.

Es importante mencionar que al hacer seguimiento a los arreglos que las entidades hicieron a los problemas presentados, se pudieron evidenciar cambios importantes, algunos derivados directamente de la corrección de las vulnerabilidades informadas, y otros surgidos de la conciencia que se apropió sobre la importancia de la seguridad y la protección de la privacidad de las personas usuarias. Los sistemas informáticos que fueron objeto de los análisis de Karisma, son más seguros ahora gracias a que reportamos las fallas que encontramos.





En conclusión

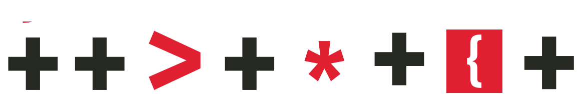
Si bien lo más obvio que resulta de nuestro análisis es que hay un problema con el diseño e implementación de las APIs aquí mencionadas, es claro que esto es un síntoma de los problemas de fondo en los métodos de desarrollo de software en estas entidades. Es necesario trabajar para que el desarrollo de sistemas que gestionen datos personales no sea tomado a la ligera, que se fortalezcan los controles de calidad, se implementen metodologías de gestión de riesgos, métodos claros de respuesta a incidentes y modelos de amenazas.

Las entidades públicas deben comprometerse a no desplegar prototipos como si fueran soluciones robustas y a desarrollar buenas prácticas en materia de información a las autoridades y posibles víctimas cuando se reportan vulnerabilidades.

Todos estos elementos deberían ser requisitos indispensables para programar soluciones que estarán al servicio del Estado y, sobre todo, de las personas que las usarán.

++++

Con el fin de aportar a un entorno más seguro con datos y acciones, a partir de este año Karisma enviará la recopilación anual de los análisis realizados en materia de seguridad digital y privacidad a la Delegatura de Protección de Datos de la Superintendencia de Industria y Comercio, al ColCERT y a la Coordinación GIT de Seguridad y Privacidad de la Información del Ministerio TIC.



Fundación
Karisma

karisma.org.co
Twitter: @Karisma
Facebook: @fundacionkarismaa
Instagram: @karismacol